

CLAIMS:

1. A method of associating data with users involving associations between user identifying information and data,
5 characterized in that concealing data is used to conceal a user identity in the user identifying information, such that it is possible to check for a given user identity whether the association applies to it.
- 10 2. The method according to claim 1, wherein the user identity is concealed using a hash function.
3. The method according to claim 1, wherein the user identity is concealed using encryption.
15 4. The method according to claim 1, wherein the concealing data comprises a random value.
5. The method according to claim 1, wherein the associations are publicly
20 available.
6. The method according to claim 1, further comprising the step of providing an association.
25 7. The method according to claim 1, further comprising the step of receiving a request for an association, and the step of providing the association.

8. The method according to claim 6, further comprising the step of signing the provided generated association.

9. The method according to claim 7, wherein the request includes the user
5 identifying information in which the user identity is concealed (step 32) using concealing data.

10. Method according to claim 1, wherein the concealing data is encrypted by a secret user key.

11. Method according to claim 1, wherein said concealing data remains fixed for reissued associations.

12. Method according to claim 1, wherein the association is a digital certificate.

15. 13. Method according to claim 12, wherein the digital certificate is an SPKI authorization certificate.

14. Method according to claim 12, wherein the association includes the right to
20 access purchased digital content.

15. 16. Method according to claim 1, wherein the association comprises a content identifier.

25 16. Method according to claim 1, wherein the association comprises a rights attributes data field.

17. Method according to claim 1, wherein the association includes an index indicating the right user identifying information associated with the user.

30 18. Method according to claim 1, further comprising the step of sending a request in relation to said data including the concealed user identifying information (step 32).

19. Method according to claim 18, wherein the request includes the concealing data in order to enable revealing of the user identifying information.

20. Method according to claim 18, wherein the request further includes a secret
5 security identifier.

21. Method according to claim 18, further including the step of encrypting the concealing data by using a secret domain key, such that the concealing data is encrypted in at least the request.

10 22. Method of giving a user access to information in relation to an association between a user and data including the steps of:

receiving from a user a request concerning said data using user identifying information related to the user, (steps 42; 50; 60; 98; 84),

15 retrieving the association including user identifying information that has been concealed using concealing data, (steps 43; 53; 77; 85; 99),

checking the concealed user identifying information in the association, (steps 44; 54; 78; 90; 104), and

20 providing the user with information related to the data, (steps 46; 56; 80; 92; 108) based on a correspondence between the concealed user identifying information in the association and user identifying information at least linked to the user.

23. Method according to claim 22, wherein the step of providing the user with information comprises providing the user access to content corresponding to said data, (steps 25 46; 56; 80; 92; 108).

24. Method according to claim 22, further including the step of performing authentication of the user (steps 40; 48; 58; 82; 94).

30 25. Method according to claim 22, wherein the user identifying information received from the user is the same as the user identifying information in the association and the step of providing is based on a correspondence between the concealed user identifying information and the user identifying information received from the user.

26. Method according to claim 22, wherein the user identifying information received from the user is different than the user identifying information in the association and further including the step of:

5 comparing the user identifying information of the user against a user domain certificate including user identifying information related to all users in a domain, (steps 52; 72),

wherein the step of checking concealed user identifying information in the association with user identifying information (steps 54; 78) is performed on user identifying information in the domain certificate, and

10 the step of providing (steps 56; 80) is performed based on a correspondence between the concealed user identifying information in the association and any user identifying information in the domain certificate.

27. Method according to claim 26, wherein the domain certificate includes

15 concealed user identifying information of all the users in the domain and an encryption of a concatenation of all user identifying information in the domain using a secret domain key.

28. Method according to claim 27, further including the steps of sending the encrypted concatenation of all user identifying information to the user (step 74) and receiving 20 identifying information about all users in the domain from said user (step 76).

29. Device (112) for hiding the identity of a user in an association between said user and data arranged to:

25 conceal user identifying information using concealing data for provision of the concealed user identifying information in the association.

30. Device (20, 22, 24) for giving a user access to information in relation to an association between a user and data arranged to:

receive a request from a user concerning said data including user identifying 30 information relating to the user,

retrieve an association between the data and a user including user identifying information, which has been concealed using concealing data,

check the concealed user identifying information in the association, and

provide the user with information related to the data based on a correspondence between the concealed user identifying information in the association and user identifying information at least linked to the user.

5 31. Device (20, 22, 24) for obtaining information in relation to an association between a user and said data arranged to:

receive user identifying information related to a user that has been concealed using concealing data, and

10 send a request concerning said data including the concealed user identifying information,

so that an association between the user and said data comprising the concealed user identifying information can be received.

15 32. Device (26) for providing information in relation to data while concealing the identity of at least one user in relation to an association between the user and said data arranged to:

receive a request concerning said data including the user identifying information which has been concealed using concealing data, and

20 provide an association between the user and said data comprising the concealed user identifying information.

33. Computer program product (110) for giving a user access to information in relation to an association between a user and data, to be used on a computer comprising a computer readable medium having thereon:

25 computer program code means, to make the computer execute, when said program is loaded in the computer:

upon reception from the user of a request related to said data using user identifying information related to the user,

30 retrieve an association between a user and said data including user identifying information that has been concealed using concealing data,

check the concealed user identifying information in the association, and

provide the user with information related to the data based on a correspondence between the concealed user identifying information in the association and user identifying information at least linked to the user.

34. Computer program product (112) for hiding the identity of a user in an association between said user and data , to be used with a computer comprising a computer readable medium having thereon:

5 computer program code means, to make the computer execute, when said program is loaded in the computer:

conceal user identifying information using concealing data for provision of the concealed user identifying information in the association.

10 35. Computer program product (110) for providing information in relation to data while concealing the identity of at least one user in relation to an association between the user and said data, to be used with a computer comprising a computer readable medium having thereon:

15 computer program code means, to make the computer execute, when said program is loaded in the computer:

provide an association between the user and said data comprising user identifying information that has been concealed using concealing data.

20 36. A data signal (114) for use in relation to data (cr_id) and comprising an association between a user (PK) and said data, which association (UR) includes user identifying information (PK) that has been concealed using concealing data (RAN).